⑲日本国特許庁(JP)　⑪特許出願公開

⑫公開特許公報(A)　平4−117826

⑤1Int.Cl.⁵　識別記号　庁内整理番号　⑬公開　平成4年(1992)4月17日

H 04 L 9/28
G 09 C 1/00

7922−5L
7117−5K　H 04 L 9/02　A

審査請求　未請求　請求項の数 1　(全7頁)

⑤4発明の名称　認証機能付き鍵配送方式

⑳特　願　平2−237498
㉒出　願　平2(1990)9月7日

⑦2発明者　松崎　なつめ　大阪府門真市大字門真1006番地　松下電器産業株式会社内
⑦2発明者　原田　俊治　大阪府門真市大字門真1006番地　松下電器産業株式会社内
⑦2発明者　館林　誠　大阪府門真市大字門真1006番地　松下電器産業株式会社内
⑦1出願人　松下電器産業株式会社　大阪府門真市大字門真1006番地
⑦4代理人　弁理士　小鍛治　明　外2名

明　細　書

1. 発明の名称

認証機能付き鍵配送方式

2. 特許請求の範囲

重複しない固有の識別情報を持った第1、第2の端末と、端末間を結ぶ通信路と、各端末が生成した公開情報に署名を施して証明書を発行するセンターとからなるシステムにおいて、証明書の発行時は、前記第1の端末は秘密情報x1を生成し、システムで公開の数pとpを法とする剰余環の原始元gを用いてx1をべきとし前記pを法とするgのべき乗剰余値y1を算出し、このy1を第1の公開情報としてセンターに通知し、前記第2の端末は秘密情報x2を生成し、x2をべきとし前記pを法とするgのべき乗剰余値y2を算出し、このy2を第2の公開情報としてセンターに通知し、センターは前記第1、2の公開情報に端末の識別情報を含めて、署名を施して証明書を生成し、各端末それぞれに配付し鍵配送時、前記第1の端末は、前記通信路に接続し、前記センターから配付された第1の端末の証明書を格納して、通信路を通じて第2の端末に送信する第1の証明書格納手段と、乱数r1を生成する第1の乱数発生手段と、前記第1の乱数発生手段と前記通信路に接続し、前記r1をべきとし前記pを法とするgのべき乗剰余値C1を算出して、前記通信路を通じて第2の端末にデータC1を送信する第1の送信データ生成手段から構成され、前記第2の端末は、前記通信路に接続し、前記センターから送信された第2の端末の証明書を格納して、通信路を通じて第1の端末に送信する第2の証明書格納手段と、前記第1の端末から送信された第1の端末の証明書から第1の端末の第1の公開情報y1を求める第1の公開情報算出手段と、乱数r2を生成する第2の乱数発生手段と、前記第2の乱数発生手段と前記通信路に接続し、前記r2をべきとし前記pを法とするgのべき乗剰余値C2を算出して、前記通信路を通じて第1の端末にデータC2を送信する第2の送信データ生成手段と、前記第2の端末の秘密情報x2を格納する第1の秘密情報格納手段と、前記第1の秘密情報格納手段と前記第

2の乱数発生手段と前記通信路に接続し、前記乱数r2と第2の端末の秘密情報x2の和をべきとし、前記pを法とする前記送信データC1のべき乗剰余値R2を算出し、前記通信路を通じて第1の端末にデータR2を送信する第3の送信データ生成手段から構成され、前記第1の端末は、前記第2の端末から送信された第2の端末の証明書から第2の端末の公開情報y2を求める第2の公開情報算出手段と、前記第2の公開情報算出手段と前記第1の乱数発生手段と前記通信路に接続し、前記乱数r1をべきとし前記pを法とする前記C2とy2の積のべき乗剰余値を求め、これと前記第2の端末から送信された第3の送信データR2を比較してこれらが同じであることによって第2の端末を認証する第1の認証手段と、前記第1の端末の秘密情報x1を格納する第2の秘密情報格納手段と、前記第2の秘密情報格納手段と前記第1の乱数発生手段と前記通信路に接続し、前記乱数r1と第1の端末の秘密情報x1の和をべきとし、前記pを法とする前記第2の送信データC2のべき乗剰余値R1を算出し、前記通信路

を通じて第2の端末にデータR1を送信する第4の送信データ生成手段と、前記第1の乱数発生手段と前記通信路に接続し、乱数r1をべきとし前記pを法とする前記第2の端末から送信された第2の送信データC2のべき乗剰余値を、前記第2の端末との共有鍵とする第1の共有鍵生成手段から構成され、前記第2の端末は、前記第1の公開情報算出手段と前記第2の乱数発生手段と前記通信路に接続し、前記乱数r2をべきとし前記pを法とする前記C1とy1の積のべき乗剰余値を求め、これと前記第1の端末から送信された第4の送信データR1を比較してこれらが同じであることによって第1の端末を認証する第2の認証手段と、前記第2の乱数発生手段と前記通信路に接続し、乱数r2をべきとし前記pを法とする前記第1の端末から送信された第1の送信データC1のべき乗剰余値を前記第1の端末との共有鍵とする第2の共有鍵生成手段から構成される認証機能付き鍵配送方式。

3. 発明の詳細な説明

産業上の利用分野

本発明は、互いにチャレンジとレスポンスをやり取りすることによって相手を認証し、その結果秘密の共有鍵を得る認証機能付き鍵配送方式に関する。なお、相手からのレスポンスの正当性確認に用いる相手端末の公開情報は、信頼のおけるセンターがあらかじめ生成した証明書によって保証されている。

従来の技術

暗号系に秘密鍵暗号方式を用いる場合、各通信対で対ごとに異なった鍵を秘密に共有する必要がある。従来の集中鍵配送方式では、鍵共有のたびに、ネットワーク上にある鍵配送センターが各共有鍵を生成し、端末に秘密に配送する必要があるため、鍵配送センターに鍵負担が集中し、端末数の多い大規模ネットワークには適していない。一方、鍵の配送と同時に、鍵を共有する相手をきちんと認証することも要望されている。したがって、ここでは認証機能を組み込んだ分散型の鍵配送方

式について説明する。分散型の鍵配送方法として、1976年にディフィとヘルマン(Diffe、Hellman)によって提案されたディエイチ（ＤＨ）鍵配送方式がある。詳細については、アイイーイーイー・トランザクションズ・オン・インフォメーション・セオリー(IEEE Trans. Inf. Theory IT-22, 6, pp644～654(Nov. 1976))を参照すること。ＤＨ鍵配送方式は有限体GF(p)上での離散対数問題が難しいことに安全性の根拠をおいている。ここではこれに認証機能を組み込んだ方法について説明する。認証を可能とするため、信頼のおけるセンター発行の証明書を用いる。

ＤＨ鍵配送方式（第1の従来例）

以下、この第1の従来例の手順を、センターによる証明書の発行のフェーズと、端末1と端末2の間の鍵配送のフェーズに分けて説明する。

＜証明書の発行フェーズ＞

（1）システムの構築時、素数pとGF(p)の原始元gを決定し各端末に公開する。ここで安全性を確保するため、pは例えば512ビット程度の大きな素

数に決定する。

（２）端末１は秘密情報x1を生成して、y1=g^x1 modpを計算する。

なお、ここで'X modp'は値Xをpで除した時の剰余を示す。

（３）端末１はy1と名前、住所など自分を特定できる情報（識別情報、又はＩＤ情報と称する）ＩＤ1を信頼のおけるセンターに送信し、証明書を請求する。

（４）センターは端末１の正当性を調べ、センターだけが知っている秘密変換fを用いて、証明書Cert1を生成し、例えば磁気カード等に格納して端末１に配付する。

Cert1=f(y1||ＩＤ1)

ここで、||は連結を示している。なお、秘密変換fの逆変換hはシステムにおいて公開であるとする。従って、Cert1を得た任意の端末はh(Cert1)を計算することで、センターによって保証された端末１の公開情報y1を得ることができる。端末２についても同様に証明書Cert2を発行する。

＜鍵配送フェーズ＞

（１）端末１は自身の証明書Cert1を端末２に、端末２は自身の証明書Cert2を端末１にそれぞれ配送する。

（２）端末１はh(Cert2)-y2||ＩＤ2を計算し、自分の秘密情報x1を用いて、

K12-y2^x1 modp-g^x1x2 modp

を求める。

（３）一方、端末２はh(Cert1)-y1||ＩＤ1を計算し、自分の秘密情報x2を用いて、

K21-y1^x2 modp-g^x1x2 modp

を求める。なお、K12-K21は端末１と２の間の共有鍵である。

ところで、暗号通信で用いられる暗号鍵は、安全上時々変更することが望ましい。上記で述べたＤＨ鍵配送方式では共有鍵を変更するのにもう１度センターに依頼して証明書を発行してもらう必要があり、非常に手間である。

第２の従来例

特開昭61-30829では、証明書は変更せずに共有

鍵を変更する方法が提案されている。証明書の発行フェーズは第１の従来例と同じである。第２図に鍵配送フェーズの手順を示している。端末1、2間の動作を以下に示す。

（１）端末１は次のようにして配送情報Z12を生成し、これと自分の証明書Cert1を端末２に送付する。

(a)乱数r1を発生する。

(b)Z12-y1^r1 modp　　…(1)

（２）端末２は次のようにして配送情報Z21を生成し、これと自分の証明書Cert2を端末１に送付する。

(a)乱数r2を発生する。

(b)Z21-y2^r2 modp　　…(2)

また、端末１から送付されてきた情報を用いて、以下のとおり端末１との共有鍵K21を生成する。

(a)Cert1より、h(Cert1)-y1||ＩＤ1を計算し、センターの認めた端末１の公開情報y1を得る。

(b)端末１からの配送情報Z12より次のように共有鍵を算出する。

K21-(Z12×y1^r2)^x2 modp　…(3)

（３）端末１は、端末２から送付されてきた情報を用いて、以下のとおり端末２との共有鍵共有鍵K12を生成する。

(a)Cert2より、h(Cert2)-y2||ＩＤ2を計算し、センターの認めた端末２の公開情報y2を得る。

(b)端末２からの配送情報Z21より次のように共有鍵を算出する。

K12-(Z21×y2^r1)^x1 modp　…(4)

なお、端末１における共有鍵K12と端末２における共有鍵生成手段K21は(1)～(4)式より同じ値になる。

K12-(Z21×y2^r1)^x1 modp-(y2^x2^r1)^x1 modp-g^x1x2x1r1r2 modp

K21-(Z12×y1^r2)^x2 modp-(y1^x2^r1)^x2 modp-g^x1x2r1r2 modp

発明が解決しようとする課題

第１の従来例では、特定の２者間の鍵が毎回同じであるという欠点がある。第１の従来例で毎回の鍵を変更するためには、センターにおいて端末

の証明書を作り替えてもらわなくてはならず、かなり手間がかかる。また、第2の従来例では証明書を変更せずに毎回の鍵を変更することができる。但し、この方式における認証機能は間接的な認証であり、自分の認識している相手とのみ同じ鍵を共有できることが保証されているというものであった。従って、きちんと相手からのデータにより相手を認証するものではない。さらに共有鍵を得るには、配送データの生成に1回、共有鍵の生成に2回の計3回のべき乗剰余演算が必要である。

本発明の認証機能付き鍵配送方式は、上述の問題点に鑑みて試みられたもので、証明書を変更せずに毎回の鍵を変更する鍵配送方式であって、さらに、相手にデータ（チャレンジ）を与え、その応答（レスポンス）によってきちんと相手を確認する認証機能を付加した鍵配送方式を提供することを目的とする。なお、この際に従来の間接的認証を付加した方法に比べて計算量の増加を最小限とする。

課題を解決するための手段

前記目的を達成するために、本発明における認証機能付き鍵配送方式は、重複しない固有の識別情報を持った第1、第2の端末と、端末間を結ぶ通信路と、各端末が生成した公開情報に署名を施して証明書を発行する信頼のおけるセンターからなるシステムにおいて、証明書の発行時は、前記第1の端末は秘密情報x1を生成し、システムで公開の数pとpを法とする剰余環の原始元gを用いてx1をべきとし前記pを法とするgのべき乗剰余値y1を算出し、このy1を第1の公開情報としてセンターに通知し、前記第2の端末は秘密情報x2を生成し、x2をべきとし前記pを法とするgのべき乗剰余値y2を算出し、このy2を第2の公開情報としてセンターに通知し、センターは前記第1、2の公開情報に端末の識別情報を含めて、署名を施して証明書を生成し、各端末それぞれに配付し、鍵配送時、前記第1の端末は、前記通信路に接続し、前記センターから配付された第1の端末の証明書を格納して、通信路を通じて第2の端末に送信する第1

の証明書格納手段と、乱数r1を生成する第1の乱数発生手段と、前記第1の乱数発生手段と前記通信路に接続し、前記r1をべきとし前記pを法とするgのべき乗剰余値C1を算出して、前記通信路を通じて第2の端末にデータC1を送信する第1の送信データ生成手段から構成され、前記第2の端末は、前記通信路に接続し、前記センターから送信された第2の端末の証明書を格納して、通信路を通じて第1の端末に送信する第2の証明書格納手段と、前記第1の端末から送信された第1の端末の証明書から第1の端末の第1の公開情報y1を求める第1の公開情報算出手段と、乱数r2を生成する第2の乱数発生手段と、前記第2の乱数発生手段と前記通信路に接続し、前記r2をべきとし前記pを法とするgのべき乗剰余値C2を算出して、前記通信路を通じて第1の端末にデータC2を送信する第2の送信データ生成手段と、前記第2の端末の秘密情報x2を格納する第1の秘密情報格納手段と前記第1の秘密情報格納手段と前記第2の乱数発生手段と前記通信路に接続し、前記乱数r2と第2の端末の

秘密情報x2の和をべきとし、前記pを法とする前記送信データC1のべき乗剰余値R2を算出し、前記通信路を通じて第1の端末にデータR2を送信する第3の送信データ生成手段から構成され、前記第1の端末は、前記第2の端末から送信された第2の端末の証明書から第2の端末の公開情報y2を求める第2の公開情報算出手段と、前記第2の公開情報算出手段と前記第1の乱数発生手段と前記通信路に接続し、前記乱数r1をべきとし前記pを法とする前記C2とy2の積のべき乗剰余値を求め、これと前記第2の端末から送信された第3の送信データR2を比較してこれらが同じであることによって第2の端末を認証する第1の認証手段と、前記第1の端末の秘密情報x1を格納する第2の秘密情報格納手段と、前記第2の秘密情報格納手段と前記第1の乱数発生手段と前記通信路に接続し、前記乱数r1と第1の端末の秘密情報x1の和をべきとし、前記pを法とする前記第2の送信データC2のべき乗剰余値R1を算出し、前記通信路を通じて第2の端末にデータR1を送信する第4の送信データ生成手

段と、前記第１の乱数発生手段と前記通信路に接続し、乱数r1をべきとし前記pを法とする前記第２の端末から送信された第２の送信データC2のべき乗剰余値を、前記第２の端末との共有鍵とする第１の共有鍵生成手段から構成され、前記第２の端末は、前記第１の公開情報算出手段と前記第２の乱数発生手段と前記通信路に接続し、前記乱数r2をべきとし前記pを法とする前記C1とy1の積のべき乗剰余値を求め、これと前記第１の端末から送信された第４の送信データR1を比較してこれらが同じであることによって第１の端末を認証する第２の認証手段と、前記第２の乱数発生手段と前記通信路に接続し、乱数r2をべきとし前記pを法とする前記第１の端末から送信された第１の送信データC1のべき乗剰余値を前記第１の端末との共有鍵とする第２の共有鍵生成手段から構成される。

作用

第２の端末は第１の端末の出力するチャレンジデータC1に対するレスポンスR2を、自分の秘密情報x2と自分の生成した乱数r2を用いて生成する。

従って、このレスポンスは正規の第２の端末しか生成することができない。第１の端末はこのレスポンスを、第２の端末の証明書から得た正規の公開情報y2によって認証する。また、レスポンスに自分の生成した秘密の乱数r2を含めているため、第１の端末および第３者はレスポンスから第２の端末の秘密情報x2を得ることはできない。同様に端末２はチャレンジデータC2に対するレスポンスR1により端末１を認証する。そして互いに相手を認証した後、相手からのチャレンジデータを用いて共有鍵を求める。

実施例

第１図は、本発明の認証機能付き鍵配送方式の鍵配送フェーズにおけるプロトコルを示す。証明書発行フェーズは従来例と同じである。

（１）端末１は次のようにして配送情報C1を生成し、これと自分の証明書Cert1を端末２に送付する。

(a)乱数r1を発生する。

(b)C1=g^r1 modp

（２）端末２は次のようにして配送情報C2を生成する。

(a)乱数r2を発生する。

(b)C2=g^r2 modp

また、前記C1に対するレスポンスとして以下のR2を生成する。そして自分の証明書CERT2とともに前記C2,R2を第１の端末に送信する。

R2=C1^r2*x2 modp

（３）端末１は端末２から送信された証明書Cert2から

h(Cert2)-y2‖I D2

を計算し、センターが認めた端末２の公開鍵y2を得る。次に、この公開鍵y2を用いて、

R2-(C2×y2)^r1 modp

が成り立つことを確かめる。もし成り立てば、通信相手が端末２であることを認証し、次の計算で端末２との共有鍵を求める。異なっていれば、この鍵配送プロトコルを取りやめる。

K12-C2^r1 modp

また、前記第２の端末からチャレンジC2に対す

るレスポンスとして以下のR1を生成する。そして第１の端末に送信する。

R1-C2^r1*x1 modp

（４）端末２は端末１から送信された証明書Cert1から

h(Cert1)-y1‖I D1

を計算し、センターが認めた端末１の公開鍵y1を得る。次に、この公開鍵y1を用いて、

R1-(C1×y1)^r2 modp

が成り立つことを確かめる。もし成り立てば、通信相手が端末１であることを認証し、次の計算で端末１との共有鍵を求める。異なっていれば、この鍵配送プロトコルを取りやめる。

K21-C1^r2 modp

なお、K12-K21-g^r1×r2 modpである。

この実施例において、相手からチャレンジに対するレスポンスを生成するためには、正規の秘密情報が必要である。そして、このレスポンスをセンターの認めた公開情報を用いて確認する。このため、この方法は直接的な相手認証を含んだ鍵配

送方式であるといえる。なお、鍵の共有は相手からうけたチャレンジを用いＤＨ鍵配送方式と同様にして行なう。また、鍵共有までの計算量については以下の通り評価する。なお、計算量の評価はべき乗剰余演算の回数を行なう。これは、安全性を確保する（公開情報から端末の秘密情報を得ることを困難にする）ために各計算の法pの数を大きく（例えば512ビット）取ると、べき乗剰余演算が全体の計算時間のネックとなるためである。双方の端末ともに、

・チャレンジの生成に１回
・レスポンスの生成に１回
・相手のレスポンスの正当性確認に１回
・共有鍵の生成に１回

の計４回のべき乗剰余演算が必要である。従って、従来の間接的な認証機能が付加された鍵配送方式に比べてわずか１回のべき乗剰余演算が増加しているだけである。なお、この実施例では、チャレンジとレスポンスを用いた認証を鍵配送と合わせて構成したが、認証方式単独として取り扱ってもよいことは言うまでもない。

発明の効果

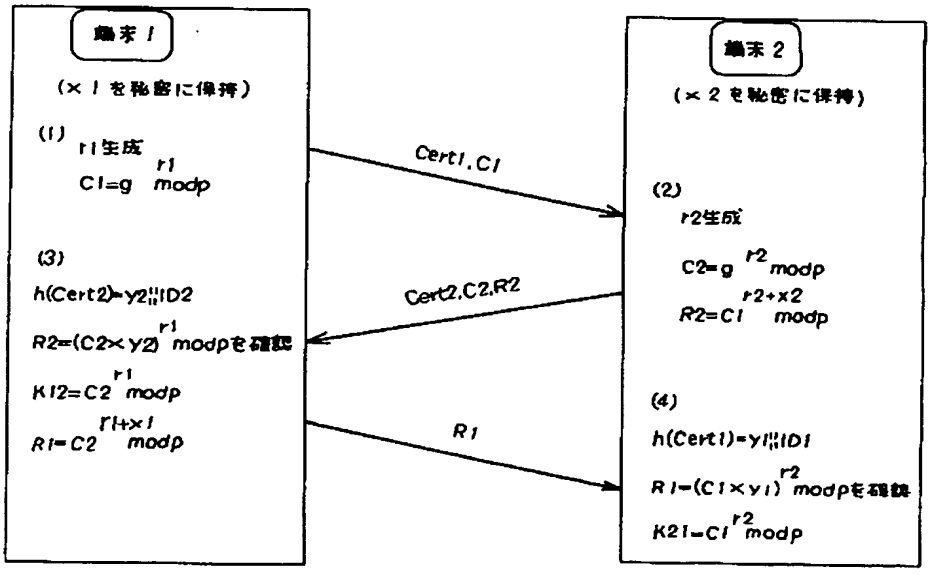
以上の説明から明らかなように本発明は、証明書を変更せずに毎回の共有鍵を変更することができる。また、相手を自身が発したチャレンジに対する応答を、センターの認めた相手の公開鍵を用いて直接的に確認する。チャレンジとレスポンスによる相手認証では、レスポンスに秘密の乱数を含めることによって端末の秘密情報を保護している。また、これにかかる計算量はべき乗剰余演算４回であり、間接的な認証しかできなかった従来の鍵配送方式と比べても最小限の計算量の増加となっている。

4. 図面の簡単な説明

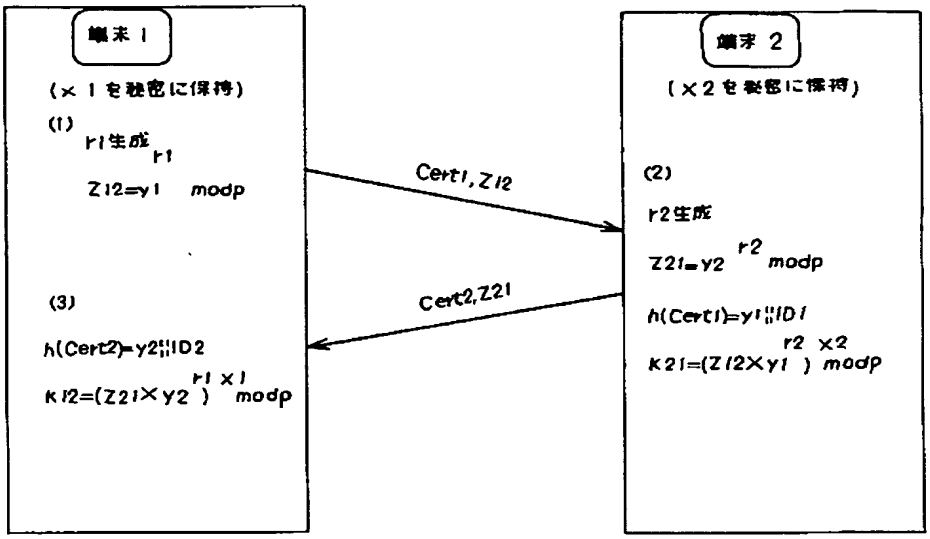
第１図は本発明の認証機能付き鍵配送方式における一実施例の鍵配送フェーズプロトコル図、第２図は従来における鍵配送フェーズプロトコル図である。

代理人の氏名　弁理士　小鍜治　明　ほか２名

第　１　図



第 2 図


端末 1
(x 1 を秘密に保持)
(1)
r1生成
Z12=y1^r1 modp
(3)
h(Cert2)=y2||ID2
K12=(Z21×y2^r1×1) modp
Cert1, Z12
Cert2, Z21
端末 2
(x2 を秘密に保持)
(2)
r2生成
Z21=y2^r2 modp
h(Cert1)=y1||ID1
K21=(Z12×y1^r2×2) modp